UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ASHLEA BERNARD, on behalf of herself and all others similarly situated, Plaintiff, v. **ONIX GROUP, LLC** Defendant.	Case No. 2:23-CV-02556 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Ashlea Bernard ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Onix Group, LLC ("Onix" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Onix for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' personally identifiable information ("PII") and protected health information ("PHI"), including names, Social Security numbers, scheduling, billing, and clinical information (collectively, "Private Information"), from criminal hackers.

2. Onix, which is based in Kennett Square, operates in the hospitality, commercial real estate development and healthcare industries.[1] The Data Breach (defined below) impacted its

[1] *See* https://www.onixgroup.com/about-onix/ (last visited on July 3, 2023).

following groups: Addiction Recovery Systems, Cadia Healthcare, Physician's Mobile X-Ray, Onix Group, and Onix Hospitality Group.[2]

3. According to a notification letter Onix posted on its website, Onix experienced a "ransomware incident" on March 27, 2023 affecting its internal computer systems between the period of March 20 and 27, 2023, which resulted in unauthorized access to Private Information (the "Data Breach").

4. Plaintiff and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

5. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, names, Social Security numbers, birthdates, and unspecified "clinical information" regarding care at one of Onix's affiliated entities. The compromised files also contained information maintained for human resources purposes, including names, Social Security numbers, direct deposit information, and health plan enrollment information.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

[2] *See* Sample Onix Individual Notification Letter, available at https://www.onixgroup.com/wpcontent/uploads/2023/05/Onix-Notice-of-Data-Security-Incident.pdf (last accessed July 3, 2023).

7. There has been no assurance offered by Onix that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

8. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

9. Plaintiff brings this class action lawsuit to address Onix's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

10. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Onix, and thus Onix was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

11. Upon information and belief, Onix failed to properly implement security practices with regard to the computer network and systems that housed the Private Information.

12. Plaintiff's and Class Members' identities are now at risk because of Onix's negligent conduct as the Private Information that Onix collected and maintained is now in the hands of data thieves and other unauthorized third parties.

13. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

14. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, breach of fiduciary duty, and declaratory and injunctive relief.

II. PARTIES

15. Plaintiff Ashlea Bernard is, and at all times mentioned herein was, an individual citizen of the State of Pennsylvania. She provided her PII and PHI to Addiction Recovery Services, one of Onix's affiliated groups, and was notified via letter dated May 26, 2023 that her information was compromised in the Data Breach.

16. Upon receipt of Plaintiff Bernard's Private Information, Addiction Recovery Services entered it into Onix's database wherein it was stored and maintained. In maintaining Plaintiff's Private Information, Onix expressly and impliedly promised to safeguard it. However, Onix did not take proper care of Plaintiff Bernard's Private Information, leading to its exposure as a direct result of its inadequate security measures.

17. Defendant Onix Group LLC is a Pennsylvania-based real estate company that provides management and consulting services to other businesses. Onix owns and operates eight hotels under franchise agreements as well as several healthcare-related businesses. Onix has a principal place of business located at 150 Onix Drive, Kennett Square, PA 19348.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Onix. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over Onix because Onix operates in and/or is incorporated in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Onix has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Onix's Business and Collection of Plaintiff's and Class Members' Private Information

21. The Onix Group was established in 1987 "for the purpose of owning, developing and operating various real estate investments principally for its own account – while also providing management and consulting services to others."[3] It operates eight hotels (with three more under development) and claims to manage "a diverse collection of commercial real estate, including commercial shopping centers, office buildings, retail pad sites and residential properties."[4]

22. The Onix Group also has a healthcare division which operates addiction recovery clinics, skilled nursing facilities, a pharmacy and a physician group in the Mid-Atlantic region.[5]

23. As a condition of providing services to the company's healthcare division, Onix requires that individuals, like Plaintiff, entrust it with their PII and PHI.

24. Due to the highly sensitive and personal nature of the information Onix acquires and stores with respect to its patients and other individuals, Onix, upon information and belief, promises to, among other things: keep the Private Information it collects and maintains private; comply with industry standards related to data security and the maintenance of the Private Information it collects and maintains; inform customers and patients of its legal duties relating to

[3] *See* https://www.onixgroup.com/about-onix/ (last visited July 3, 2023).
[4] *Id*.
[5] *See* https://www.onixgroup.com/businesses/ (last visited on July 3, 2023).

data security and comply with all federal and state laws protecting the Private Information entrusted to it; only use and release the Private Information it maintains for reasons that relate to the services it provides; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Onix assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

26. Plaintiff and Class Members relied on Onix to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members

27. According to the notice sent to Plaintiff by Addiction Recovery Systems in or around late May, Onix experienced a ransomware incident on March 27, 2023 that affected its internal computer systems. A subsequent investigation revealed that unauthorized cybercriminals had access to Onix's network between March 20 and March 27, 2023, and that the threat actors "corrupted certain systems, and removed a subse4t of files."

28. Through the Data Breach, the unauthorized cybercriminals accessed a cache of highly sensitive Private Information, including PHI and Social Security numbers.

29. Onix had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

30. Plaintiff and Class Members provided their Private Information to Onix with the reasonable expectation and mutual understanding that Onix would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

31. Onix's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

32. Onix knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

33. As a HIPAA covered business entity (*see infra*), Onix was on notice that companies operating within the healthcare industry are required to implement adequate safeguards to prevent unauthorized use or disclosure of private information, and that such companies are susceptible targets for data breaches.

34. Onix was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[6]

35. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

[6] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on July 3, 2023).

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[7]

36. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] In 2022, the largest growth in compromises occurred in the healthcare sector.[9]

37. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[10]

38. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and

---

[7] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on July 3, 2023).

[8] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on July 3, 2023).

[9] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on July 3, 2023).

[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on July 3, 2023).

identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[11]

39. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[12]

40. Due to the nature of Onix's business, which includes a healthcare division, Onix knew, or should have known, the importance of safeguarding patient Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Onix's patients as a result of a breach. Onix failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Onix Failed to Comply with HIPAA

41. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

---

[11] *Id*.

[12] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on July 3, 2023).

42. Onix's Data Breach resulted from a combination of insufficiencies that indicate Onix failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Onix's Data Breach that Onix either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

43. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

44. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

45. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

46. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

47. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

48. Based upon Defendant's Notice to Plaintiff and Class Members, Onix reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

49. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

50. Onix reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

51. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

52. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

53. Onix reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

54. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

55. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

56. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for

recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

57. In addition, Onix's Data Breach could have been prevented if Onix had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

58. Onix's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Onix creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

59. Because Onix has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure Onix's approach to information security is adequate and appropriate going forward. Onix still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

E. Onix Failed to Comply with FTC Guidelines

60. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and

appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

61. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

62. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. As evidenced by the Data Breach, Onix failed to properly implement basic data security practices. Onix's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

65. Onix was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Onix Failed to Comply with Industry Standards

66. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

67. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Onix include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

68. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

69. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Onix Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

71. In addition to its obligations under federal and state laws, Onix owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Onix owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

72. Onix breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Onix's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

73. Onix negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

74. Had Onix remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

75. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Onix.

H. Onix Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

76. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such

as data breaches or unauthorized disclosure of data.[13] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

77. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

78. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

79. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

[13] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on July 3, 2023).

Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

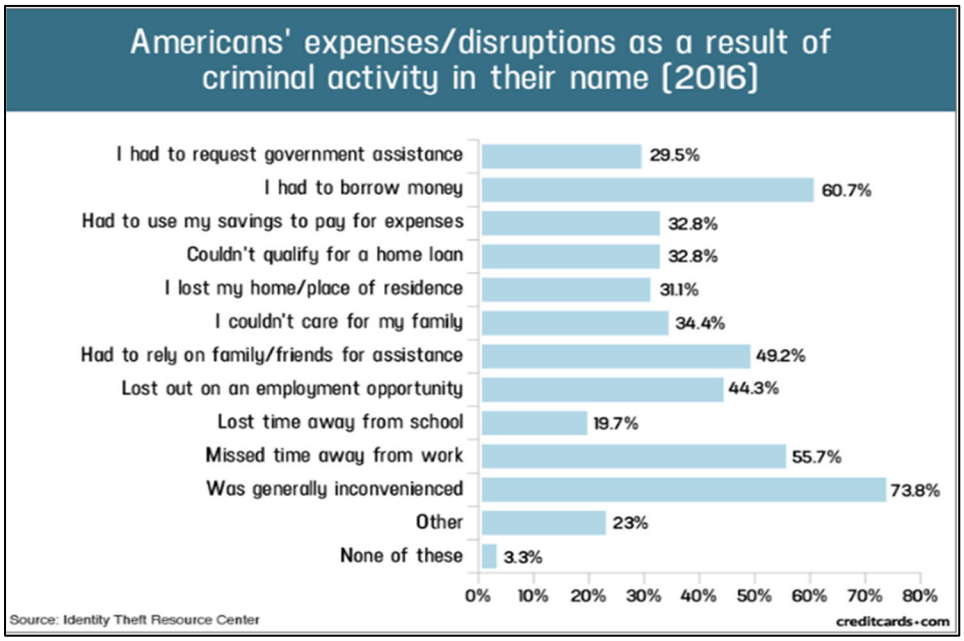
80. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

81. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[14] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

82. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[14] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited July 3, 2023).

83. In fact, a study by the Identity Theft Resource Center[15] shows the multitude of harms caused by fraudulent use of PII:



84. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[16]

85. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

86. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[17]

---

[15] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on July 3, 2023).

[16] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on July 3, 2023).

[17] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on July 3, 2023).

87. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

88. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

89. The ramifications of Onix's failure to keep its patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

90. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

91. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on July 3, 2023).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[19]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

92. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

93. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiff's and Class Members' Damages

94. Onix received Plaintiff's Private Information in connection with providing certain devices to them. In requesting and maintaining Plaintiff's Private Information for business purposes, Onix expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's Private Information. Onix, however, did not take proper care of Plaintiff's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Onix's inadequate data security measures.

95. On or around May 26, 2023, Addiction Recovery Systems sent Plaintiff a notice concerning the Onix Data Breach. The letter stated that the Data Breach may have resulted in

[19] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited July 3, 2023).

unauthorized access to Plaintiff's Private Information stored on Onix's systems. The notice stated that the compromised information that was present on the impacted files may have included names, Social Security numbers, scheduling, treatment, and billing information, and that such information was "removed" from Onix's corrupted systems.

96. Onix's negligent conduct, which allowed the Data Breach to occur, caused Plaintiff significant injuries and harm, including but not limited to, the following—Plaintiff immediately devoted (and must continue to devote) time, energy, and money to: closely monitoring her medical statements, bills, records, and credit and financial accounts; changing login and password information on any sensitive account even more frequently than she already does; more carefully screening and scrutinizing phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; searching for suitable identity theft protection and credit monitoring services and paying for such services to protect herself; and placing fraud alerts and/or credit freezes on her credit file. Plaintiff has taken or will be forced to take these measures in order to mitigate her potential damages as a result of the Data Breach.

97. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years, and possibly her entire life. Consumer victims of data breaches are more likely to become victims of identity fraud.

98. Plaintiff greatly values her privacy, especially while receiving healthcare services. Plaintiff and Class Members did not receive the full benefit of their bargain when paying for medical services (or when payments were made on their behalf), and instead received services that were of a diminished value to those described in their agreements with their respective healthcare institutions that had made agreements with Onix for the benefit and protection of Plaintiff and

Class Members and their respective Private Information. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

99. Plaintiff and Class Members would not have obtained medical services and/or devices from Onix, or paid the amount they did to receive such, had they known that Onix would negligently fail to adequately protect their Private Information. Indeed, Plaintiff paid Onix for medical devices with the expectation that Onix would keep her Private Information secure and inaccessible from unauthorized parties. Plaintiff and Class Members would not have obtained services from their medical providers had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

100. Plaintiff and Class Members have lost confidence in Onix, as a result of the Data Breach.

101. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff's and Class members' Private Information as detailed above, and Plaintiff and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

102. Plaintiff is also at a continued risk of harm because her Private Information remains in Onix's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Onix fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

103. As a result of the Data Breach, and in addition to the time Plaintiff has spent and anticipates spending to mitigate the impact of the Data Breach on her life, Plaintiff has also suffered emotional distress from the public release of her Private Information, which she believed would be protected from unauthorized access and disclosure. The emotional distress she has experienced includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her Private Information for the purposes of identity theft and fraud.

104. Additionally, Plaintiff has suffered damage to and diminution in the value of her highly sensitive and confidential Private Information—a form of property that Plaintiff entrusted to Onix and which was compromised as a result of the Data Breach Onix failed to prevent. Plaintiff has also suffered a violation of her privacy rights as a result of Onix's unauthorized disclosure of her Private Information.

105. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

106. Each Class Member received a cryptically written notice letter from Defendant stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this Private Information could have gone, or who might have access to it.

107. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

108. Thus, as a direct and proximate result of Onix's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

109. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

110. Specifically, Plaintiff proposes the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States whose Private Information was impacted as a result of the Data Breach, including all who were sent a notice of the Data Breach.

111. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

112. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

113. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

114. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of over 300,000 patients and customers of Onix whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Onix's records, Class Members' records, publication notice, self-identification, and other means.

115. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Onix engaged in the conduct alleged herein;

b. Whether Onix's conduct violated the FTCA and/or HIPAA;

c. When Onix learned of the Data Breach

d. Whether Onix's response to the Data Breach was adequate;

e. Whether Onix unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Onix failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Onix's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Onix's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Onix owed a duty to Class Members to safeguard their Private Information;

j. Whether Onix breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Onix had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Onix breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Onix knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Onix's misconduct;

p. Whether Onix's conduct was negligent;

q. Whether Onix's conduct was *per se* negligent;

r. Whether Onix was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

116. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Onix. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

117. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

118. Predominance. Onix has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Onix's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

119. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Onix. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

120. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Onix has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

121. Finally, all members of the proposed Class are readily ascertainable. Onix has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Onix.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

122. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

123. Onix knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

124. Onix knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Onix was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

125. Onix owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Onix's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

126. Onix's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

127. Onix's duty also arose because Defendant was bound by industry standards to protect its patients' confidential Private Information.

128. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Onix owed them a duty of care not to subject them to an unreasonable risk of harm.

129. Onix, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Onix's possession.

130. Onix, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

131. Onix, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

132. Onix breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

133. Onix acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

134. Onix had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Onix with their Private Information was predicated on the understanding that Onix would take adequate security precautions. Moreover, only Onix had the ability to protect its systems (and the Private Information that it stored on them) from attack.

135. Onix's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein and as already admitted in the notice letters sent to Plaintiff.

136. Onix's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

137. As a result of Onix's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

138. Onix also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

139. As a direct and proximate result of Onix's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

140. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

141. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

142. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Onix to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

143. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

144. Pursuant to Section 5 of the FTCA, Onix had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

145. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Onix had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

146. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning

meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

147. Onix breached its duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

148. Specifically, Onix breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

149. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Onix's duty in this regard.

150. Onix also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

151. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Onix's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

152. Plaintiff and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Onix's failure to comply with both constitutes negligence *per se*.

153. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Onix's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

154. As a direct and proximate result of Onix's negligence *per se*, Plaintiff and the Class have suffered, and/or are at a substantial and imminent risk of suffering, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the actual misuse of their Private Information and the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

155. As a direct and proximate result of Onix's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

156. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Onix to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

157. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

158. Plaintiff and the Class Members entered into implied contracts with Onix under which Onix agreed to safeguard and protect Plaintiff's and Class Members' Private Information and to timely and accurately notify Plaintiff and Class Members that such Information had been breached and compromised.

159. Plaintiff and the Class were required to, and delivered, their Private Information to Onix as part of the process of obtaining services provided by Onix.

160. Plaintiff and Class Members paid money, or money was paid on their behalf, to Onix in exchange for services.

161. Onix solicited, offered, and invited Class Members to provide their Private Information as part of Onix's regular business practices. Plaintiff and Class Members accepted Onix's offers and provided their Private Information to Onix.

162. Onix accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services for Plaintiff and Class Members.

163. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Onix whereby Onix became obligated to reasonably safeguard Plaintiff's and Class Members' Private Information.

164. In delivering their Private Information to Onix and paying for healthcare services, Plaintiff and Class Members intended and understood that Onix would adequately safeguard the data as part of that service.

165. Upon information and belief, in its written policies, Onix expressly and impliedly promised to Plaintiff and Class Members that they would only disclose protected information and other Private Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

166. The implied promise of confidentiality includes consideration beyond those preexisting general duties owed under HIPAA or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

167. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

168. Plaintiff and Class Members would not have entrusted their Private Information to Onix in the absence of such an implied contract.

169. Had Onix disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Onix.

170. Onix recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

171. Plaintiff and Class Members fully performed their obligations under the implied contracts with Onix.

172. Onix breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

173. As a direct and proximate result of Onix's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

174. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

175. This Count is pleaded in the alternative to Count III above.

176. Upon information and belief, Onix funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

177. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Onix.

178. Plaintiff and Class Members conferred a monetary benefit on Onix. Specifically, they purchased medical services from Onix and/or its agents and in so doing provided Onix with their Private Information. In exchange, Plaintiff and Class Members should have received from Onix the services that were the subject of the transaction and have their Private Information protected with adequate data security.

179. Onix knew that Plaintiff and Class Members conferred a benefit which Onix accepted. Onix profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

180. Plaintiff and Class Members conferred a monetary benefit on Onix, by paying Onix as part of rendering medical services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Personal Information, and by providing Onix with their valuable Personal Information.

181. Onix was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Onix instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Onix's failure to provide the requisite security.

182. Under the principles of equity and good conscience, Onix should not be permitted to retain the money belonging to Plaintiff and Class Members, because Onix failed to implement appropriate data management and security measures that are mandated by industry standards.

183. Onix acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

184. If Plaintiff and Class Members knew that Onix had not secured their Personal Information, they would not have agreed to provide their Private Information to Onix.

185. Plaintiff and Class Members have no adequate remedy at law.

186. As a direct and proximate result of Onix's conduct, Plaintiff and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private

Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Onix's possession and is subject to further unauthorized disclosures so long as Onix fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

187. As a direct and proximate result of Onix's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

188. Onix should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Onix should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Onix's services.

COUNT V
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

189. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

190. In light of the special relationship between Onix and its patients, whereby Onix became a guardian of Plaintiff's and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) Onix was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of Plaintiff and Class

Members. This benefit included (1) the safeguarding of Plaintiff's and Class Members' Private Information; (2) timely notifying Plaintiff and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Onix's patients' Private Information was and is stored.

191. Onix had a fiduciary duty to act for the benefit of Plaintiff and the Class upon matters within the scope of its relationship with its patients, in particular, to keep the Private Information secure.

192. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to diligently investigate and discovery the Data Breach to determine the number of Class Members affected.

193. Onix breached its fiduciary duties to Plaintiff and the Class by failing to protect their Private Information.

194. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Onix created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

195. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

196. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

197. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

198. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

199. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

200. Onix breached its fiduciary duties to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

201. Onix breached its fiduciary duties to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

202. As a direct and proximate result of Onix's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

203. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

204. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws, regulations, and industry standards described in this Complaint.

205. Onix owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

206. Onix still possesses Private Information regarding Plaintiff and Class Members.

207. Plaintiff alleges that Onix's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromises of her Private Information will occur in the future.

208. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Onix owes a legal duty to secure its patients' Private Information and to timely notify customers of a data breach under the common law, HIPAA, and the FTCA;

b. Onix's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patients' and customers' Private Information; and

c. Onix continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

209. This Court should also issue corresponding prospective injunctive relief requiring Onix to employ adequate security protocols consistent with legal and industry standards to protect patients' Private Information, including the following:

a. Order Onix to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Onix must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Onix's systems on a periodic basis, and ordering Onix to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Onix's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Onix's customers and patients should take to protect themselves.

210. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Onix. The risk of another such breach is real, immediate, and substantial. If another breach at Onix occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

211. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Onix if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Onix's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Onix has a pre-existing legal obligation to employ such measures.

212. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Onix, thus preventing future injury to Plaintiff and other patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Onix to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Onix to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: July 3, 2023 Respectfully submitted,

/s/ Nicholas Sandercock

Nicholas Sandercock
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: nsandercock@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com